

# ENCIPHERING DEVICE AND METHOD FOR INPUT BIT STRING

**Patent number:** JP10262041  
**Publication date:** 1998-09-29  
**Inventor:** KOBAYASHI YOSHINAO; OBA NOBUYUKI; MUNETO SEIJI  
**Applicant:** INTERNATL BUSINESS MACH CORP <IBM>  
**Classification:**  
- international: H04L9/10; H04L9/08  
- european:  
**Application number:** JP19970059480 19970313  
**Priority number(s):**

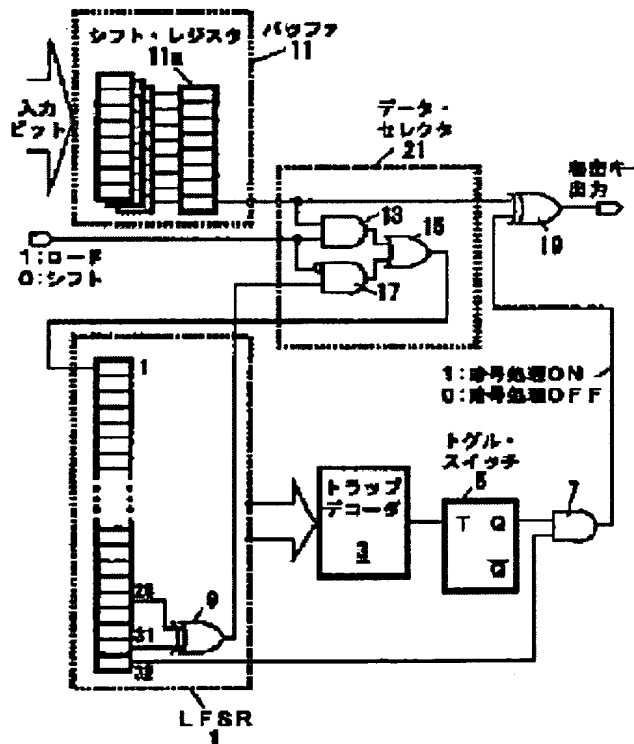
**Also published as:**

 US6282291 (B1)

## Abstract of JP10262041

**PROBLEM TO BE SOLVED:** To non-specifically execute the exposure/non-exposure mode of a secret key by outputting a presumable bit string, in response to the input of an initial bit string and performing the switching between the enciphering processing and the output processing of input bit strings, when the output of a prescribed trap bit string is detected.

**SOLUTION:** When an initial bit string is loaded into an LFSR (linear feedback shift register) 1, a trap decoder 3 starts its operation to monitor the bit of the LFSR 1. When a trap bit string is detected, the decoder 3 outputs a switch signal and a toggle switch 5 inverts its own output. Then the output of the LFSR 1 continuously serves as the input of an exclusive OR circuit 19, until the decoder 3 outputs a switch signal. At the same time, the output of a shift register 11a undergoes the exclusive OR processing (enciphering processing) by means of a pseudo-random number, i.e., the output of the LFSR 1. Meanwhile, the output of the register 11a is used as it is, when the decoder 3 outputs a switch signal.



Data supplied from the **esp@cenet** database - Patent Abstracts of Japan

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-262041

(43) 公開日 平成10年(1998) 9月29日

(51) Int.Cl.<sup>6</sup>

H 0 4 L 9/10

9/08

識別記号

F I

H 0 4 L 9/00

6 2 1 A

6 0 1 A

審査請求 未請求 請求項の数10 OL (全 7 頁)

(21) 出願番号 特願平9-59480

(22) 出願日 平成9年(1997) 3月13日

(71) 出願人 390009531

インターナショナル・ビジネス・マシーンズ・コーポレーション

INTERNATIONAL BUSINESS MACHINES CORPORATION

アメリカ合衆国10504、ニューヨーク州  
アーモンク (番地なし)

(72) 発明者 小林 芳直

神奈川県大和市下鶴間1623番地14 日本アイ・ビー・エム株式会社 東京基礎研究所内

(74) 代理人 弁理士 合田 潔 (外2名)

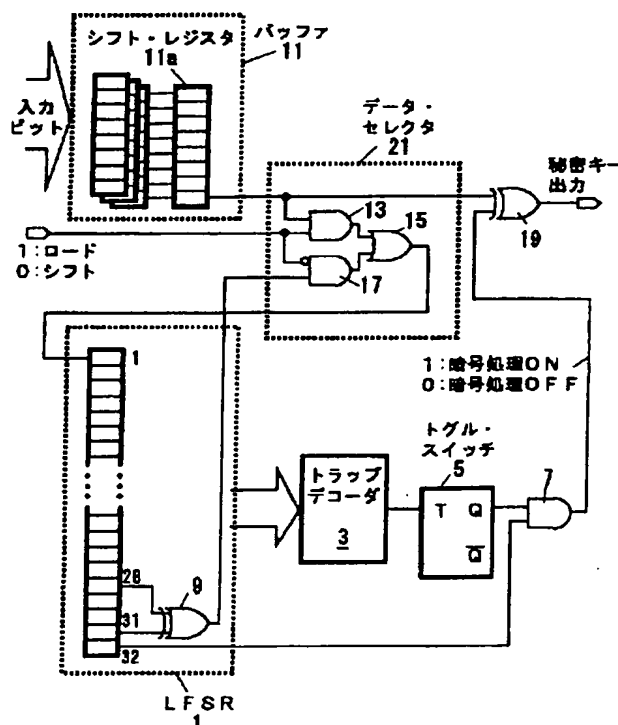
最終頁に続く

(54) 【発明の名称】 入力ビット列暗号化装置及び方法

(57) 【要約】

【課題】 秘密キーを露出させるモードと露出させないモードを非明示的に実行可能とする装置及び方法を提供する。

【解決の手段】 初期ビット列の入力にตอบสนองして、初期ビット列から予想可能なビット列を出力するビット列出力手段と、ビット列出力手段が所定のトラップ用ビット列を出力することを検出した場合には、スイッチ信号を出力するスイッチ信号出力手段と、スイッチ信号の受信にตอบสนองして、ビット列出力手段からのビット列を用いて入力ビット列を暗号化する処理と、入力ビット列を出力する処理を切り換えるスイッチとを含む。



#### 【特許請求の範囲】

【請求項 1】初期ビット列の入力に応答して、前記初期ビット列から予想可能なビット列を出力するビット列出力手段と、

前記ビット列出力手段が所定のトラップ用ビット列を出力することを検出した場合には、スイッチ信号を出力するスイッチ信号出力手段と、

スイッチ信号の受信に応答して、前記ビット列出力手段からのビット列を用いて入力ビット列を暗号化する処理と、前記入力ビット列を出力する処理を切り換えるスイッチとを含む入力ビット列暗号化装置。

【請求項 2】前記ビット列出力手段が、リニア・フィードバック・シフト・レジスタであることを特徴とする請求項 1 記載の入力ビット列暗号化装置。

【請求項 3】前記所定のトラップ用ビット列が前記ビット列出力手段により出力されるような初期ビット列と、出力されないような初期ビット列とを選択可能にする手段をさらに含む請求項 1 記載の入力ビット列暗号化装置。

【請求項 4】前記スイッチ信号出力手段が、前記所定のトラップ用ビット列を前記リニア・フィードバック・シフト・レジスタが保持しているか判断する手段を含むことを特徴とする請求項 2 記載の入力ビット列暗号化装置。

【請求項 5】前記ビット列出力手段が所定数のビットを出力した後に、前記入力ビット列を入力することを特徴とする請求項 1 記載の入力ビット列暗号化装置。

【請求項 6】前記暗号化する処理が、排他的論理和回路により実施されることを特徴とする請求項 1 記載の入力ビット列暗号化装置。

【請求項 7】前記入力ビット列が、秘密キーであることを特徴とする請求項 1 記載の入力ビット列暗号化装置。

【請求項 8】初期ビット列を入力するステップと、前記初期ビット列の受信に応答して、前記初期ビット列から予想可能なビット列を 1 ビットずつ出力するビット列出力ステップと、

前記ビット列出力ステップにより 1 ビット出力されるごとに、所定のトラップ用ビット列が出力されるかどうか判断する判断ステップと、

前記所定のトラップ用ビット列が出力されると判断された場合、暗号化を実施する処理と暗号化を実施しない処理とを切り換えるステップとを含む入力ビット列暗号化方法。

【請求項 9】前記暗号化を実施する処理は、前記初期ビット列から予想可能なビット列を用いて実行されることを特徴とする請求項 8 記載の入力ビット列暗号化方法。

【請求項 10】初期ビット列の入力に応答して、前記初期ビット列から予想可能なビット列を出力するビット列生成器と、

前記ビット列生成器が所定のトラップ用ビット列を出力

することを検出した場合には、スイッチ信号を出力するスイッチ信号生成器と、

スイッチ信号の受信に応答して、前記ビット列生成器からのビット列を用いて入力ビット列を暗号化する処理と、前記入力ビット列を出力する処理を切り換えるスイッチとを含む入力ビット列暗号化装置。

#### 【発明の詳細な説明】

##### 【0001】

【発明の属する技術分野】本発明は、暗号化装置及び方法に関し、より詳しくは、暗号化に用いられるキーを必要に応じて暗号化して又は平文で出力できるようにする装置及び方法に関する。

##### 【0002】

【従来の技術】暗号には秘密のキー（鍵）を用いる方式がある。例えば、公開鍵方式である RSA（Rivest, Shamir and Adelman）や、秘密鍵方式の DES（Data Encryption Standard）でも秘密キーを用いる。当然、秘密キーは他人に知られないようにして、秘密キーの盗用を防がなければならない。よって、秘密キーそのものを半導体チップ内の ROM（Read Only Memory）に格納するような方法では、チップの解析により秘密キーを特定されてしまうおそれがあり、好ましくない。

【0003】この解決方法としては、LFSR（Linear Feedback Shift Register）により秘密キーを生成する方法があるが、秘密キーのビット数分の LFSR を必要とするため、ハードウェアのコストが大きくなってしまいうという欠点がある。

【0004】一方、RSA の暗号化装置は、ある数の素数判定にも用いることができる。この素数判定は、RSA における秘密キーが素数でなければならぬため行われる。この素数判定では、秘密キーは露出している必要がある。もし、同じ暗号化装置を素数判定と暗号化の両方に用いる場合、秘密キーを露出させるモードと露出させないモードを設ける必要があるが、このモードの切り分けを明示的に行うと秘密キーを盗み取ろうとする者に大きなヒントを与えることになり、得策ではない。

##### 【0005】

【発明が解決しようとする課題】以上の事項に鑑み、本発明の目的は、秘密キーを露出させるモードと露出させないモードを非明示的に実行可能とする装置及び方法の提供を目的とする。

【0006】また、上記装置及び方法により、秘密キーを盗み取ろうとする者に有効に対抗することを目的とする。

##### 【0007】

【課題を解決するための手段】上記本発明の目的は、以下のような装置により達成される。すなわち、初期ビット列の入力に応答して、初期ビット列から予想可能なビット列を出力するビット列出力手段と、ビット列出力手段が所定のトラップ用ビット列を出力することを検出し

た場合には、スイッチ信号を出力するスイッチ信号出力手段と、スイッチ信号の受信にตอบสนองして、ビット列出力手段からのビット列を用いて入力ビット列を暗号化する処理と、入力ビット列を出力する処理を切り換えるスイッチを含む装置である。このビット列出力手段は、先に述べたLFSRを用いることができる。しかし、ビット数は先のように大きくする必要はない。またこの場合、スイッチ信号出力手段は、所定のトラップ用ビット列をLFSRが保持しているか判断するようにすることもできる。但し、出力したビット列を検査していても同様の効果を奏することができる。

【0008】また、非明示的にモードの変換を実施するのに、所定のトラップ用ビット列がビット列出力手段により出力されるような初期ビット列と、出力されないような初期ビット列とを選択可能にすることによって可能となる。外部から観察している者は、いつトラップ用ビット列が発生してスイッチ信号が出力されるか分からないので、初期ビット列を分けることは明示的なモードの切替を示すものではない。

【0009】また、ビット列出力手段が所定数のビットを出力した後に、入力ビット列を入力するようにすることもできる。秘密キーを用いる後処理に合わせて入力ビット（秘密キー）を入力すればよい。さらに、この所定数のビットの間にトラップ用ビット列が出力されるように初期値を決定すれば、モード切替後の処理が簡単になる。

【0010】先に示した暗号化する処理は、排他的論理和回路により実施されるようにすることもできる。よって、排他的論理和された後のビット列が真の秘密キーとなるよう、入力データを用意する必要がある。

【0011】以上述べた事項を、半導体チップの回路や、ソフトウェア等により実施することは、以下の詳細な説明を読めば明らかになる。

【0012】

【発明の実施の形態】本発明の回路図を図1に示す。入力されるビット列は最初にバッファ11に格納されるようになっており、バッファ11には4つのレジスタが用意されている。このうちの1つのレジスタはシフトレジスタ11aであり、その下位ビットがAND回路13及び排他的論理和回路19に接続されている。このバッファ11内の構成は一例であって、このような構成に限定されない。例えば、処理すべき入力ビット列（秘密キー）及び後に説明する初期ビット列を全て格納するようなメモリを用意しておき、記憶しているビットを1ビットずつ出力するような装置でもよい。また、このバッファ11は、外部とのインターフェースが8ビットであり且つ後段のLFSR1が32ビット必要とするため、8ビットのレジスタを4つ含んでいるが、外部とのインターフェースはどのようなビット数でもよく、またLFSR1のビット数も32ビットである必要はないので、そ

れぞれの条件に合わせてバッファ11の構成を変化させることができる。また、バッファ11は、LFSR1及び排他的論理和回路19の後処理の動作に合わせてビットを出力することができればよいので、LFSR1のビット数に合わせなくともよい場合もある。

【0013】AND回路13のもう一つの入力、図示しない制御回路からの出力が接続されている。また、この制御回路からの出力は、NOT回路を介してAND回路17に接続されている。このAND回路17の他方の入力には、LFSR9内の排他的論理和回路9の出力が接続されている。そして、AND回路13及びAND回路17の出力は、OR回路15の入力に接続され、このOR回路15の出力はLFSRの第1ビットに接続されている。LFSR1の各ビット（ここでは31ビットのみ。但し、トラップ・デコーダ3が必要とするビットのみでもよい。）はトラップ・デコーダ3に接続されている。トラップ・デコーダ3は、トグル・スイッチ5に接続されている。トグル・スイッチ5の出力（正の出力）は、AND回路7に接続されている。このAND回路7のもう1つの入力、LFSR1の出力ビット（ここでは32ビット目）に接続されている。このAND回路7の出力は、排他的論理和回路19のもう1つの入力として接続されており、この排他的論理和回路19の出力が、秘密キー出力となる。排他的論理和回路9の入力は、LFSR1が非常に長い周期の擬似乱数を発生するようにレジスタ段を選択して接続する。この図では、28段目と31段目を接続している。なお、AND回路13及び17、及びOR回路15を合わせてデータセクタ21となる。

【0014】図1の回路の動作を説明する前に、LFSR1について説明する。LFSR1は、先に示したように排他的論理和回路9の入力を適切に選択すれば、非常に長い周期の擬似乱数を発生する。31ビットのLFSR1であれば、 $2^{31}-1$ （図1のLFSR1の32ビット目は出力のみに使っているので、実質31ビットのLFSRである。また、全てのビットが0である場合はLFSRがロックされるので除く。）の周期で擬似乱数を発生する。よって、図2に示したように $2^{31}-1$ 個のビット列のうち、任意の位置の31ビット以上の初期ビット列（例えば初期ビット列1、2）を決めると、その後のビット列は予想可能となる。本発明はこの性質を用いる。

【0015】では、図1の回路の動作を説明する。初めに、LFSR1の初期ビット列をロードする。このロードの際には、図示しない制御回路はその出力を論理“1”にして、AND回路17の出力を論理“0”に保ち（NOT回路を介しているため）、AND回路13の出力がそのままLFSR1の第1ビットに入るようにする。よって、シフトレジスタ11aの出力をそのままLFSR1の第1ビットに入力できるようになる。バッファ11で

は、シフトレジスタ11aのビットを1ビットずつ出力し、シフトレジスタ11aが空になると、他のレジスタにためておいたビットをシフトレジスタ11aにそのまま1回で渡す。この動作を、LFSR1に初期ビット列が充填されるまで繰り返す。

【0016】図1では32ビットの初期ビット列がLFSR1に充填された後、図示しない制御回路はその出力を論理“0”にする。そうすると、AND回路13の1つの入力が論理“0”となるのでAND回路13は論理“0”のみ出力するようになる。一方、AND回路17の入力は論理“1”になるので（NOT回路を介しているため）、AND回路17のもう1つの入力が、そのまま出力されることとなる。よって、OR回路15を介して、AND回路17のもう1つの入力である排他的論理和回路9の出力がLFSR1の第1ビットに入力されるようになる。これで、初期ビット列以降のビット列をLFSR1が出力する状態となった。

【0017】この状態で、LFSR1の31ビットを監視するトラップ・デコーダ3が動作を開始する。トラップ・デコーダ3は、予め決められたトラップ用ビット列をLFSR1が出力するかを監視するものである。もし、トラップ・デコーダ3は、このトラップ用ビット列を検出した場合には、スイッチ信号を出力する。トラップ用ビット列を検出しなければ、スイッチ信号を出力しない。スイッチ信号を出力すると、トグル・スイッチ5は自身の出力を反転させる。すなわち、論理“0”を出力していれば論理“1”に、論理“1”を出力していれば論理“0”を出力するようになる。トグル・スイッチ5の初期値が論理“1”であるとする、AND回路7の出力はスイッチ信号をトグル・スイッチ5が受信するまで、LFSR1の出力となる。一方、スイッチ信号をトグル・スイッチ5が受信すると、AND回路7の1つの入力が論理“0”に変わるため、LFSR1の出力はAND回路7から出力されない。

【0018】よって、スイッチ信号をトラップ・デコーダ3が出力するまでは、LFSR1の出力が排他的論理和回路19の1つの入力になるため、シフトレジスタ11aの出力が、LFSR1の出力である擬似乱数で排他的論理和处理（暗号化处理）される。一方、スイッチ信号をトラップ・デコーダ3が出力すると、排他的論理和回路19の1つの入力は論理“0”に固定されるため、シフトレジスタ11aの出力がそのまま、排他的論理和回路19の出力となる。

【0019】ここで、トラップ用ビット列をどのように設定すべきかについて説明する。先に述べたように、秘密キーを露出させるモードと秘密キーを露出させないモードとを設ける必要がある。秘密キーを露出させるモードは、排他的論理和回路19の出力がシフトレジスタ11aの出力そのままでない、秘密キーが露出していることにはならない。よって、トグル・スイッチ5の出力

が論理“0”でなければならない。ということは、トラップ・デコーダ3からスイッチ信号が出力されている必要がある。よって、トラップ用ビット列を図2のような位置のビット列にした場合、初期ビット列としてLFSR1に最初にロードするビット列は、初期ビット列1でなければならない。すなわち、初期ビット列1を入力した後、初期ビット列1とトラップ用ビット列がLFSR1内に現れるまでの間のビット数分、LFSR1を空回りさせ、トラップ用ビット列がLFSR1内に現れてスイッチ信号がトラップ・デコーダ3から出力された後に、シフトレジスタ11aから秘密キーを出力するようにすればよい。

【0020】一方、秘密キーを露出させないモードでは、LFSR1の初期ロード用ビット列として図2の初期ビット列2を用いられればよい。この場合、初期ビット列2以降にはトラップ用ビット列は存在しない。（通常、入力データはLFSR1の出力ビット列に比して非常に短いデータであるから、周期的であるからといって元に戻るようなことはない。）よって、常にトグル・スイッチ5の出力は論理“1”になっているので、LFSR1の出力が排他的論理和回路19に入力される。よって、シフトレジスタ11aの出力は、LFSR1の擬似乱数によって排他的論理和处理（暗号化处理）される。逆に、排他的論理和回路19の出力を意味あるビット列にする場合には、シフトレジスタ11aからの入力ビットをLFSR1の出力に合わせて用意しておく必要がある。

【0021】秘密キーを露出させないモードにおいても、初期ビット列2をLFSR1にロードしてから、所定ビット空回りさせてからシフトレジスタ11aから入力ビット列を出力するようにしてもよい。これは、後処理の動作タイミングに合わせて入力ビット列を出力するようにすればよいということである。

【0022】以上は本発明の一例であるが、様々な変形が考えられる。例えば、LFSR1は、初期ビット列を設定するとそれから後のビット列が予想可能となるようにビット列を発生するような他の回路によって置換可能である。また、トラップ・デコーダ3は、LFSR1内のビットを検査してスイッチ信号を出力するような構成としたが、LFSR1の出力自体を検査してゆくような方法でも可能である。すなわち、図2のトラップ用ビット列がLFSR1内に生じるならば、そのトラップ用ビット列の前のビット列（図2の上のビット列）は既にLFSR1から出力されている。よって、出力されているビット列を監視していれば、トラップ用ビット列がLFSR1内に存在しているか否かは判別可能である。

【0023】また、ここまではトラップ用ビット列31ビットを検出した場合にスイッチ信号を出力するようなトラップ・デコーダ3を示したが、LFSR1の出力ビット列によっては、LFSR1内の決められた数のビットの状態を検査するのみでスイッチ信号を出力可能な場

合もある。また、トラップ用ビット列を1つではなく複数設定することも考えられる。例えば、秘密キーを露出させない場合、一部のみを露出させて残りを露出させないといったことも可能である。図3に示したように、初期ビット列から開始し、一旦トラップ用ビット列1以降LFSR1の出力による暗号化を停止する。その後シフトレジスタ11aから入力ビットを入力し始める。そして、トラップ用ビット列2が現れるとLFSR1の出力による暗号化を開始する。よって、トラップ用ビット列2が現れるまでシフトレジスタ11aからの入力ビットは露出されることになる。しかし、最初のうち露出している、全てが露出されているわけではなく、より動作が分かりにくくなり、盗用しにくくなる。なお、トラップ用ビット列の個数は1個2個に限定されるものではない。但し、個数を多くすると、トラップ・デコーダ3の構成が複雑になる。LFSR1を空回りさせている間に、複数回スイッチ信号を出力させるようにしたりすることも可能である。

【0024】他の変形例としては、図1では図示しない制御装置が1つの信号の切替で初期ビット列のロードと、LFSR1の動作期間とを区別するようにしているが、複数の信号にて、上記ロードとLFSR1の動作期間とを区別するように回路を構成してもよい。すなわち、データセレクト21に様々な構成が可能である。また、排他的論理和回路19によってシフトレジスタ11aからの入力ビットを暗号化しているが、排他的論理和回路以外に回路にてスクランブルするようにしてもよい。さらに、トグル・スイッチ5の出力は初期値が論理“1”であったが、初期値を論理“0”にすることも可能である。しかし、この場合には、秘密キーを露出させるモードと露出させないモードとを入れ替えて用いる必要がある。

【0025】以上の説明では、初期ビット列から所定回数LFSR1を空回りさせるような動作を説明したが、空回りさせなくともよい。但し、後段の処理と同期させるため、及びLFSR1がどのような状態の時に入力ビット（秘密キー）が暗号化されるか分かりにくくなる等、外から見て動作を分かりにくくするため、空回りは必要となる場合が多いと考えられる。

【0026】なお、上の動作をまとめると以下のように

なる。(1)最初に初期ビット列を入力する(ステップ110)。(2)LFSR1などを用いて、初期ビット列から予想可能なビット列を1ビットずつ出力する(ステップ120)。(3)先のステップで1ビット出力することに、予め決められたトラップ用ビット列が出力されるか検査する(ステップ130)。もし、トラップ用ビット列を検出しない場合には、ステップ120及び130を繰り返す。(4)もし、トラップ用ビット列を検出した場合には、入力ビットの暗号処理実施と暗号処理非実施を切り換える(ステップ140)。暗号処理を実施している場合には、暗号処理非実施に、暗号処理非実施であれば、暗号処理実施に切り換える。この処理を処理終了(ステップ150)とされるまで繰り返す。通常、入力ビット(秘密キー)がなくなったところで処理終了となる。

【0027】

【効果】秘密キーを露出させるモードと露出させないモードを非明示的に実行可能とする装置及び方法を提供することができた。

【0028】また、秘密キーを盗み取ろうとする者に有効に対抗することもできた。

【0029】また、小さいハードウェア規模により秘密キーのスクランブルも可能にできた。

【図面の簡単な説明】

【図1】本発明の回路例を示した図である。

【図2】LFSR1が出力するビット列の利用法について説明する図である。

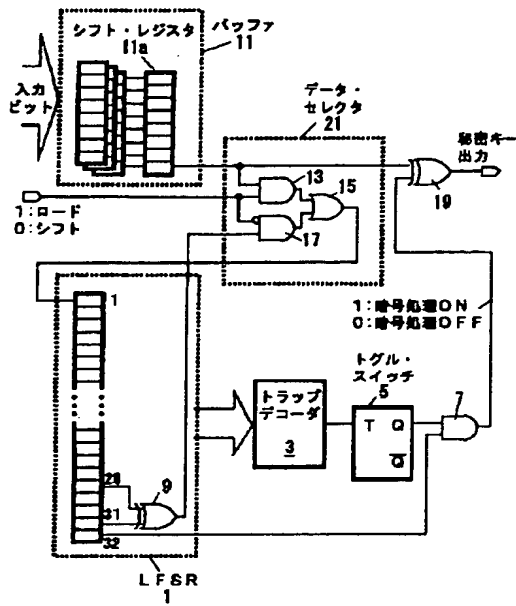
【図3】LFSR1が出力するビット列の利用法について説明する図である。

【図4】本発明の動作を説明するためのフローチャートである。

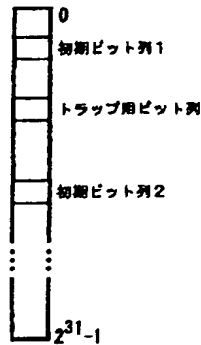
【符号の説明】

- 1 LFSR
- 3 トラップデコーダ
- 5 トグル・スイッチ
- 7、13、17 AND回路
- 9、19 排他的論理和回路
- 11 バッファ 11a シフトレジスタ
- 15 OR回路
- 21 データセレクト

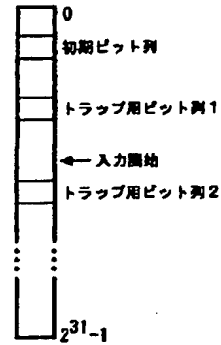
【図 1】



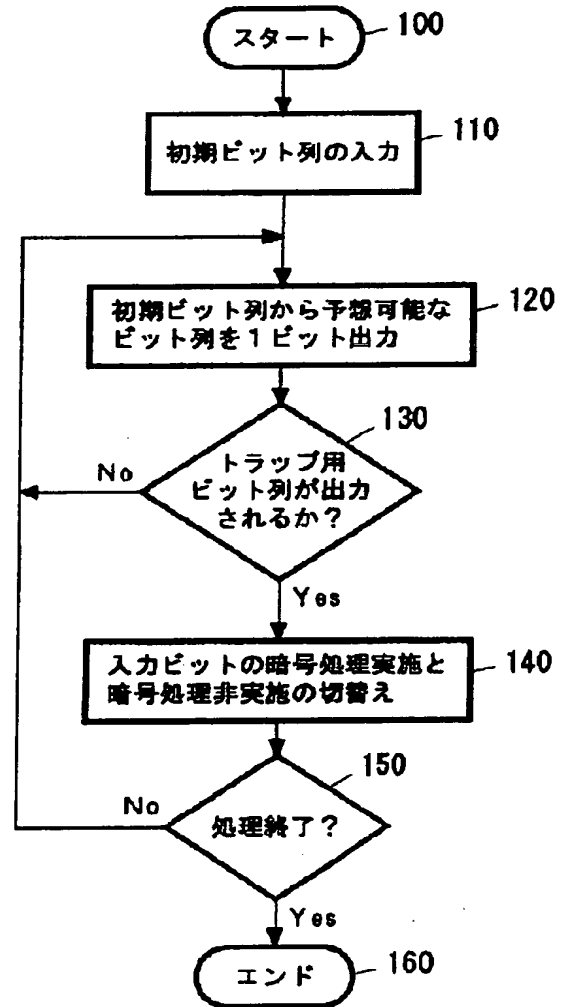
【図 2】



【図 3】



【図 4】



フロントページの続き

(72)発明者 大庭 信之  
神奈川県大和市下鶴間1623番地14 日本ア  
イ・ビー・エム株式会社 東京基礎研究所  
内

(72)発明者 宗藤 誠治  
神奈川県大和市下鶴間1623番地14 日本ア  
イ・ビー・エム株式会社 東京基礎研究所  
内